AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A method for secure communication between a first communicating party and a second communicating, comprising:

identifying a first shared random number associated with a first communicating party;

identifying a second shared random number associated with a second communicating party;

~~exchanging said first shared random number and said second shared random number between said first communicating party and said second communicating party; and~~

transmitting a first message from said second communicating party to said first communicating party, said first message including said first shared random number, and said first message being encoded with a symmetric encryption key;

transmitting a second message from said first communicating party to said second communicating party, said second message including said second shared random number, and said second message being encoded with an asymmetric encryption key: and

obtaining a shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

2. (Previously presented) The method of claim 1, wherein said combining function includes a logical function.

3. (Previously presented) The method of claim 2, wherein said logical function includes an exclusive or (XOR) function.

4. (Cancelled)

5. (Currently amended) The method of claim 1~~[[4]]~~, further comprising the step of transmitting ~~a~~ the second message from said second computer to said first computer~~, said second message including said second shared random number~~.

6. (Previously Presented) The method of claim 4, wherein said first message is encoded using an encoded password.

7. (Previously presented) The method of claim 6, wherein said encoded password is an encrypted password.

8. (Previously presented) The method of claim 6, wherein said step of encoding said first message comprises encrypting said first message using said encoded password.

9. (Previously presented) The method of claim 5, wherein said first message also includes an asymmetric key.

10-23 (Cancelled)

24. (Currently amended) A method for secure communication between a first communicating party and a second communicating party, comprising:

receiving a first message including a first shared random number from said ~~first~~ second communicating party, said first message being encoded with a symmetric encryption key;

identifying a second shared random number associated with said second communicating party, said first message being encoded with a symmetric encryption key;

transmitting ~~said~~ a second ~~shared random number~~ message to said first communicating party, said second message including a second shared random number, and said second message being encoded with an asymmetric encryption key; and

obtaining a shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

25. (Cancelled)

26. (Previously Presented) The method of claim 24, wherein said step of identifying a second shared random number comprises generating said second shared random number.

27. (Currently amended) The method of claim 24, wherein said first message is encoded using a first key obtained using information ~~obtained~~ from a password.

28. (Currently amended) The method of claim 24, wherein said first message is encoded using a first key obtained using information ~~obtained~~ from a password.

29. (Currently amended) The method of claim 24, wherein said first message is encrypted using a first key obtained using information ~~obtained~~ from a password.

30. (Previously presented) The method of claim 27, wherein said first key is obtained by encoding said password.

31. (Previously Presented) The method of claim 30, wherein encoding said password comprises encrypting said password.

32-35 (Cancelled).

36. (Currently amended) The method of claim ~~32~~23, further comprising receiving ~~said~~ a password from a user.

37. (Cancelled)

38. (Previously Presented) The method of claim 24, wherein said combining function includes an exclusive or (XOR) function.

39. (Previously presented) The method of claim 27, wherein said first key is generated using an encoded password obtained from said password.

40. (Previously presented) The method of claim 39, wherein said encoded password is an encrypted password.

41. (Previously presented) The method of claim 40, wherein said encrypted password is obtained from an output of a one-way function having an input including said password.

42. (Previously presented) The method of claim 41, wherein said one-way function is a hash function.

43. (Previously presented) The method of claim 27, further comprising the step of receiving said password from a user.

44. (Previously presented) The method of claim 43, further comprising transmitting information identifying said user.

45. (Previously presented) The method of claim 43, wherein said user is a human user.

46. (Previously presented) The method of claim 43, further comprising the step of obtaining said first key from an output of a one-way function having an input including said password.

47. (Previously presented) The method of claim 43, further comprising decrypting said first message using information obtained from said password.

48. (Previously presented) The method of claim 27, further comprising transmitting identification information for a user.

49. (Previously presented) The method of claim 27, wherein said first message also includes a second key.

50. (Previously presented) The method of claim 49, wherein said second key is an asymmetric key.

51. (Previously presented) The method of claim 50, wherein said second message is encoded with said second key.

52. (Previously Presented) The method of claim 25, wherein said second message is encrypted with said second key.

53. (Previously presented) The method of claim 51, wherein said second message also includes a timestamp.

54. (Previously presented) The method of claim 27, wherein said first message also includes a timestamp.

55. (Previously presented) The method of claim 27, wherein said first message also includes a second key and a timestamp.

56. (Previously presented) The method of claim 55, wherein said second key is an asymmetric key.

57–111 (Cancelled)

112. (Currently amended) A method for secure communication between a first communicating party and a second communicating party, comprising the steps of:

identifying a first shared random number associated with a first message from said ~~first~~ second communicating party, said first message including said first shared random number, and said first message being encoded with a symmetric encryption key;

receiving a message including a second shared random number from said ~~second~~ first communicating party, said second message being encoded with an asymmetric encryption key; ~~and~~

obtaining ~~said~~ a shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number.

113. (Currently amended) The method of claim 112, further comprising transmitting ~~a~~ the first message including said first shared random number.

114. (Previously presented) The method of claim 113, wherein said step of identifying a first shared random number comprises generating said first shared random number.

115. (Currently amended) The method of claim 113, wherein said first message is encoded using a first key.

116. (Currently amended) The method of claim 115, wherein said first message is encrypted using a first key.

117. (Currently amended) The method of claim 115, wherein said first message also includes a second key.

118. (Previously presented) The method of claim 115, wherein said first key corresponds to a password.

119. (Currently amended) The method of claim 118, wherein said first key ~~is~~ comprises an encoded password.

120. (Currently amended) The method of claim 119, wherein said first key ~~is~~ comprises an encrypted password.

121 (Cancelled)

122. (Currently amended) The method of claim ~~121~~112, wherein said combining function includes a logical function.

123. (Previously presented) The method of claim 122, wherein said logical function includes an exclusive or (XOR) function.

124-126 (Cancelled).

127. (Currently amended) The method of claim ~~125~~112, further comprising decoding said second message.

128. (Previously presented) The method of claim 127, wherein said decoding said second message comprises decoding said second message using a third key.

129. (Currently amended) The method of claim 128, wherein said third key and said ~~second~~ asymmetric encryption key form an asymmetric key pair.

130. (Previously presented) The method of claim 129, further comprising the step of generating said asymmetric key pair.

131. (Previously presented) The method of claim 130, wherein said asymmetric key pair is generated dynamically.

132. (Previously presented) The method of claim 130, wherein said asymmetric key pair is selected from a set of pre-generated asymmetric key pairs.

133. (Previously presented) The method of claim 115, further comprising receiving information identifying a user.

134. (Previously presented) The method of claim 133, wherein said first key is associated with said user.

135. (Previously presented) The method of claim 134, wherein said first key corresponds to a password known by said user.

136. (Previously presented) The method of claim 135, wherein said first key is an encoded value of said password.

137. (Previously presented) The method of claim 135, wherein said encoded value of said password is an encrypted value of said password.

138. (Previously presented) The method of claim 136, wherein said first key is a value of said password after being sent through a one-way function.

139. (Previously presented) The method of claim 136, further comprising the step of obtaining said first key by looking up said user in a password file.

140. (Previously presented) The method of claim 139, wherein said password file contains an encoded password.

141. (Previously presented) The method of claim 140, wherein said encoded password is an encrypted password.

142. (Previously presented) The method of claim 139, wherein said password file is encoded.

143. (Previously presented) The method of claim 142, wherein said encoded password file is an encrypted password file.

144-148 (Cancelled)

149. (Previously presented) The method of claim 115, wherein said first message also includes a timestamp.

150. (Previously presented) The method of claim 115, wherein said first message also includes a second key and a timestamp.

151. (Currently amended) The method of claim 150, wherein said second key ~~is~~ comprises an asymmetric key.

152. (Canceled)

153. (Cancelled)